


**PRIVILEGED AND CONFIDENTIAL
ATTORNEY-CLIENT COMMUNICATION
ATTORNEY WORK PRODUCT**

memorandum

TO	John J. Fischer, CEO, Try Safety First J. Robert Smyjunas, Jr., Chairman of the Board of Directors, Try Safety First	DATE	October 11, 2016
FROM	 Jamie Barnett, Rear Admiral (Ret.) Ian D. Volner Stephen R. Freeland	EMAIL	JBarnett@Venable.com IDVolner@Venable.com SRFreeland@Venable.com
		PHONE	(202) 344-4814 (202) 344-4695 (202) 344-4837
RE	<i>In the Matter of Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities</i> , FCC 13-58 – FCC Authority to Require Implementation of Try Safety First’s Securitized Prison Protocol Technology		

I. INTRODUCTION

On May 1, 2013, the Federal Communications Commission (“FCC”) released a Notice of Proposed Rulemaking in *In the Matter of Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, FCC 13-58 (“NPRM”), which was subsequently published in the Federal Register on June 18, 2013. *See* 78 Fed. Reg. 36469. In the NPRM, the FCC takes “steps to facilitate the development of multiple technological solutions to combat the use of contraband wireless devices in correctional facilities nationwide.” NPRM, at 3. This is because, as the FCC has concluded, “[p]risoners’ use of contraband wireless devices to engage in criminal activity is a serious threat to the safety of prison employees, other prisoners, and the general public.” *Id.* The Rulemaking proceeding is designed to “remove barriers to the deployment and viability of existing and future technologies used to combat contraband wireless devices.” *Id.*

While the NPRM discusses three (3) different technologies that existed at the time the NPRM was issued – namely, managed access, detection, and jamming – the NPRM focuses on

managed access as a potential solution for the majority of correctional facilities, seeking comment on the following proposed rules:

- Immediately processing *de facto* lease agreements or spectrum manager lease agreements for spectrum used exclusively in managed access systems in correctional facilities, and streamlining other aspects of the lease application or notification review process for those managed access systems in correctional facilities;
- Forbearing, to the extent necessary, from the individualized application review and public notice requirements of Section 308, 309, and 310(d) of the Communications Act of 1934, as amended (“the Act”), for qualifying managed access leases; and
- Establishing a presumption that managed access operators provide a private mobile radio service (“PMRS”), streamlining the process for seeking Special Temporary Authority (“STA”) to operate a managed access system, while seeking specific comment on whether to establish a requirement that managed access providers provide notice to nearby households and businesses prior to activation of a managed access system.

Id. at 3-4.

At the time the NPRM issued, the FCC was likely unaware of Try Safety First’s Securitized Prison Protocol technology which, using software installed on a wireless phone by way of an update or during manufacture, can completely disable all functions of contraband wireless devices – including voice, text, e-mail, WiFi, and camera functions – save for 911 capability. Try Safety First met with FCC staff on several occasions and has also submitted comments and *ex parte* submissions in order to educate the Commission on its Securitized Prison Protocol technology. As a result of these meetings, the FCC has indicated to Try Safety First that it intends to issue a new Notice of Proposed Rulemaking in the near future seeking comment on Try Safety First’s technology.

In anticipation of the new NPRM, as well as in response to the existing NPRM, this memorandum summarizes the limitations of the three (3) technologies discussed in the NPRM as compared to Try Safety First’s Securitized Prison Protocol technology. It also explores the various sources of FCC authority for it to require carriers or manufacturers to install Try Safety First’s software on wireless devices.

In short, Try Safety First is the only technology that provides a ubiquitous solution to the problem of contraband cell phones in correctional facilities. Moreover, this technology does not suffer from the functional limitations that persist with the three (3) alternative technologies discussed in the NPRM.

As described in more detail below, the FCC has at least two (2) independent sources of authority to require carriers and/or manufacturers to install Try Safety First's software on wireless devices. These are the: (1) FCC's Part 15 authority, which gives them regulatory authority over manufacturers of wireless devices; and (2) FCC's ancillary authority.

II. THE LIMITATIONS ON EXISTING TECHNOLOGIES AS COMPARED TO TRY SAFETY FIRST'S SECURITIZED PRISON PROTOCOL TECHNOLOGY

While each of the three (3) technologies discussed in the NPRM provide some capability to combat the contraband wireless device problem, each also have inherent limitations that prevent them from fully resolving the problem.

A. Managed Access Systems

"Managed access systems are micro-cellular, private networks that analyze transmissions to and from wireless devices to determine whether the device is authorized or unauthorized for purposes of accessing public carrier networks." NPRM, at 9. "The systems provide operational flexibility to the correctional facility administrators by allowing them to disable services without having to physically remove them." *Id.* "Authorized devices are allowed to communicate normally (*i.e.*, transmit and receive voice, text, and data) with the commercial wireless network, while transmissions to or from unauthorized devices are terminated." *Id.*

Managed access, however, is extremely expensive for correctional institutions, with costs ranging from \$1.2 million to \$5 million per facility depending on its size. *See* Try Safety First White Paper, at 7. Further, the managed access system does not disable the entire functionality of the wireless device. Functions such as camera usage and, potentially, internet access through the use of WiFi may still be used by inmates. In short, it is not a completely effective solution. Managed access systems also require approval from the FCC for each correctional facility, as well as lease agreements with spectrum licensees for each facility. This adds administrative burden and delay to attempts to solve the public safety problem.

B. Detection Systems

The NPRM also discusses two (2) forms of detection methods as potential solutions to the problem. These are detect-and-confiscate and detect-and-terminate. *See* NPRM, at 11, 26-32. "Detection systems use passive, receive-only technology and do not transmit radio signals." *Id.* at 11. "For accurate position location in an environment such as within a prison facility, detection technology triangulates a cell phone signal and requires correctional [facility] staff to physically search a small area (such as a prison cell) and seize the identified cell phone." *Id.* (quoting NTIA Report, at 27). While these systems "do not pose an interference threat to wireless operations" (*id.* at 12), they do have at least four (4) major limitations. First, the inmate is capable of using all of the device's functionality – phone, text, internet, camera, etc. – up until the time it is confiscated, to the extent it is even found and confiscated by a prison official after detection. Second, detection systems are not capable of identifying the specific location of a contraband device; they are only

capable of narrowing down the location to within three (3) to five (5) meters. *See* NPRM, at 12. Third, even if the contraband device is located, prison officials are at significant risk of physical harm while searching for and confiscating it. Fourth, a major source of contraband wireless devices in prisons are prison officials themselves, who are either threatened or bribed by inmates to smuggle the devices into and out of the facility. It is unreasonable to assume that the same officials who provided the devices to inmates in the first instance will act diligently to confiscate those devices once they are detected by the detection system.

Detect-and-terminate is another potential yet undeveloped and untested solution that is discussed in the NPRM. *See* NPRM, at 26-33. "Detection systems can operate continuously, detecting contraband devices regardless of the time of day." NPRM, at 31. The FCC is seeking "to provide flexibility to detection or related technology providers, correctional facilities, and carriers to develop systems that most effectively and efficiently terminate service to contraband wireless devices." *Id.* In doing so, the FCC seeks specific comment on a proposed system whereby a detection system would first detect a contraband wireless device as well as the carrier network on which it is operating. *See* NPRM, at 30-32. Once detected, an authorized prison official would then submit a request to the identified carrier to terminate service. *See id.* at 30-31. Assuming the carrier can verify that the device actually operates on its network, and assuming further that the carrier can authenticate the request for termination, the carrier would then have one (1) hour (or such other time as may eventually be adopted by the Commission) in which to terminate service to the detected contraband device. *See* NPRM, at 32-33.

While this proposed system would terminate wireless service to a contraband device, it, too, has several significant limitations that prevent it from adequately resolving the problem. First, as with the detect-and-confiscate system discussed above, the inmate will be able to use all functionality of the contraband device up to the time the carrier terminates wireless service to it (if it is able to do so at all). Second, there is still the chance that the person who smuggled the device into the facility is the same one that will be in charge of making the termination request, potentially reducing the likelihood that the termination request will even be made.

Third, as the comments from Verizon Wireless and AT&T demonstrate, there are several administrative and legal hurdles to the approval and implementation of a detect-and-terminate system. While Verizon Wireless "agrees that a process is needed to deal with requests by prison officials or their agents to terminate service to contraband devices," the proposed detect-and-terminate solution "embraced in part by the Commission raises a number of concerns and questions that cannot be answered at this time given the lack of experience with such requests and information about the volume of termination requests carriers might receive." July 18, 2013 Comments of Verizon Wireless, at 2. According to Verizon Wireless, these questions and concerns include, but are not limited to: (1) the accuracy of the identification (i.e., whether the device is in fact a contraband device and, if so, whether it is actually that of a Verizon Wireless subscriber) (*see id.* at 6); (2) the security of the information provided to the carrier (i.e., whether the information conveyed by the authorized requester is secure) (*see id.* at 7); (3) the timing of the termination (*see id.* at 7-8); and (4) liability protection for the carrier in the event it inadvertently

terminates the service of a non-contraband device. *See id.* at 8. Because the answers to these questions remain unknown, Verizon Wireless contends that the FCC should require that service terminations for contraband devices be done only pursuant to a court order, at least initially. *See id.* at 9. “Should experience demonstrate that a court order process is too slow or overly burdensome on prison officials or their Solutions Providers, the Commission can revisit the issue and consider a different process once all parties gain more experience with service terminations and once more detection systems are deployed.” *Id.* at 9. CTIA makes similar arguments in its initial comments. *See* July 18, 2013 Comments of CTIA – The Wireless Association®, at 11-12 (to the extent that the FCC adopts CellAntenna’s detect-and-terminate proposal, carriers should only be required to terminate service pursuant to an order from a court of relevant jurisdiction).

AT&T takes a more direct approach, arguing that the Commission is prohibited from delegating authority to request service termination to prison officials. While AT&T does not contest the Commission’s authority to directly require carriers to terminate service, AT&T contends that the FCC may not “delegate this authority to a third party, such as a corrections officer or managed access system operator” (July 17, 2013 Comments of AT&T, Inc., at 8) because the Act only “permits the FCC to delegate its functions to a ‘panel of commissioners, an individual commissioner, an employee board, or an individual employee.’” *Id.* (quoting 47 U.S.C. § 155(c)(1)). Therefore, according to AT&T, only the Commission itself or a court can order it to terminate service. *See id.* at 3. With respect to all other termination requests – including those from a prison official or managed access system provider – the carrier should retain discretion on whether to terminate service. *See id.* at 8-9.

C. Jamming

The third technology discussed in the NPRM is wireless signal jamming. “Radio signal jamming is the purposeful disruption of electronic devices, equipment, or systems via radio frequency interference.” NPRM, at 12. “A radio signal jamming device transmits on the same radio frequencies as wireless devices and base stations, disrupting the communication link between the device and the network base station, and rendering any wireless device operating on those frequencies unusable.” *Id.*

As with managed access and detection systems, jamming also has several significant limitations. First and foremost, it is illegal except in certain limited circumstances. *See* NPRM, at 12. Second, jamming has the real potential to also interfere with legitimate wireless devices operating within the range of the jamming system. As the FCC itself recognizes, “[w]hen used to disrupt wireless devices, radio signal jammers cannot differentiate between contraband devices and legitimate devices, including devices making 911 calls.” *Id.* “Radio jammers block all wireless communications on affected spectrum bands.” *Id.* In this regard, jamming systems are unnecessarily and dangerously over-inclusive.

Jamming systems are also under-inclusive, as they do not disable *all* functions of the contraband device, such as the camera.

D. The Need for a Ubiquitous Solution to Disable All Functionality of Contraband Cell Phones Except 911 Capability

As demonstrated above, the three (3) technologies discussed by the FCC will not completely disable the functionality of contraband wireless devices, will involve human intervention that may decrease the likelihood that a device is detected and confiscated or detected with carrier service termination, and/or will implicate legal and administrative issues that hinder or prevent their adoption and implementation. What is needed is a solution that is ubiquitous, disables all contraband cell phone functionality (save for 911), and which involves minimal human intervention.

Try Safety First's Securitized Prison Protocol technology provides that solution. This technology is comprised of a two part system – one part software and one part hardware. *See* Try Safety First White Paper, at 5. The software component consists of what is known as TSF Prison Protocol, which is to be loaded onto the firmware of all wireless phones in the United States. *See id.* With respect to existing phones, the software will be loaded through a USB hardwire to the manufacturer website, an over-the-air firmware update from the carrier (the quickest method) or through a website set up by Try Safety First that will be linked to manufacturer and carrier websites. *See id.* at 13. New phones will have the software installed during manufacture. *See id.*

The hardware component – known as the Protocol Trigger Device for Prisons (“PTDP”) – is a unique precision range transmitter/beacon with a one (1) to fifteen (15) meter range. *See id.* at 11. These devices are strategically placed inside the prison fences and buildings to broadcast a prison protocol trigger signal. All functionality of cell phones with the TSF Prison Protocol software – except 911 capabilities – will be disabled once inside the prison fence line and in range of the broadcast trigger signal. *See id.*

More specifically, when a cell phone is first powered up, the Try Safety First software will scan first for a PTDP. *See id.* at 10. If an active PTDP is found, the mobile device will identify its exact geographical location and then cross reference the device in order to apply proper operation in compliance with the applicable law for that jurisdiction to any phone operating inside a defined “Restricted Safety Zone” within the correctional facility. *See id.* If no active PTDP is found, the phone operates normally. *See id.* As the phone continues to scan (usually every 20 to 30 seconds) to ensure it is operating across the best or preferred network using the best or preferred base station tower, the scan will always include a search for an active PTDP and, if one is found, the contraband cell phone's functionality will be completely disabled except for 911 calls. *See id.*

Try Safety First's Securitized Prison Protocol is the only current technology that completely disables all of a cell phone's functionality – including voice, text, e-mail, Wi-Fi, and camera/video – while permitting 911 calls to connect. *See id.* This technology does so without tracking, listening to or recording any activity on the cell phone. *See id.*

III. FCC AUTHORITY

A. Authority Identified in the NPRM for Detect-and-Terminate – Section 303 – Implicates Administrative and Legal Issues

As discussed above, the NPRM expressly contemplates that one potential solution to combat contraband wireless devices in correctional facilities is detect-and-terminate. *See* NPRM, at 27. More specifically, “[c]onsistent with CellAntenna’s proposal, [the FCC] propose[s] to require CMRS licensees to terminate service to contraband devices within correctional facilities pursuant to a qualifying request from an authorized party” and seeks “comment on the costs and benefits of this proposal.” *Id.* There is an extended discussion in the NPRM that 47 U.S.C. § 303 provides the FCC with the authority to adopt this proposed detect-and-terminate rule. *See* NPRM, at 28 (FCC indicating that it “has authority under Section 303 to require CMRS providers to terminate service to contraband wireless devices.”) (citing 47 U.S.C. § 303); *see also* NPRM, at 28-29.

As Verizon, AT&T and CTIA point out, there are a number of administrative and legal problems with the FCC’s argument. *See supra* at 4-5. This memorandum, therefore, focuses on other, stronger authority for the FCC to require carriers and/or manufacturers to install Try Safety First’s software on wireless devices. This authority is summarized below.

B. The FCC’s Section 332, Part 15 and Ancillary Authority

The FCC has broad authority under Section 332 to regulate the spectrum over which wireless devices operate in order to promote the safety of life and property. More specifically, 47 U.S.C. § 332 provides, in pertinent part, as follows: “In taking actions to manage the spectrum to be made available for use by the private mobile service, the Commission shall consider, consistent with section 1 of this Act, whether such actions will . . . promote the safety of life and property.” 47 U.S.C. § 332(a)(1).

The Federal Government, several States and the FCC itself have all concluded that there is an overriding public interest in preventing prisoners from using wireless devices to further a criminal enterprise from within correctional facilities. *See* NPRM, at 3, 5. The Commission’s NPRM made efforts to address this problem. However, the problem continues to grow, largely unabated. *See, e.g.*, June 24, 2015 Letter from the American Correctional Association to Secretary Dortch (urging the FCC to “issue rulemaking regarding contraband cellphones in prisons and jail[s]” because “the problem is only getting worse.”). While a few correctional facilities have achieved some success in testing or using a managed access system (*see* NPRM, at 10-11), as described above, these systems are not capable of disabling all functionality of contraband cell phones. Moreover, the great majority of correctional facilities have not implemented any technological solutions to combat this problem, either because of cost or other resource limitations.

In May of this year, ten (10) Governors wrote to the Commission encouraging the FCC to reevaluate the FCC’s regulations regarding contraband cell phones. *See* May 23, 2016 Letter to

Chairman Wheeler from Governor Nikki Haley (SC) *et al.* In April, FCC Commissioner Pai held a field hearing in Columbia, South Carolina on combating the public safety threats posed by inmates' use of contraband cell phones. *See* Commissioner Pai's Field Hearing on Contraband Cellphones, April 6, 2016. And the FCC understands that it must take action. *See Unofficial announcement of Commission action*, February 29, 2016, Comment of Commissioner Pai ("We cannot let inmates treat prison as just another base of operations for criminal enterprises. We need to act."). New technology developed by Try Safety First now makes this possible, and no statutory bars hinder its implementation.

As demonstrated below, along with the authority discussed in the NPRM itself, the FCC has additional authority to require equipment manufactures and/or carriers to install firmware on mobile devices that would limit specific phone operations in certain locations.

1. Authority under Section 302a

The FCC already regulates mobile devices under Part 15 of its Rules, which sets out the rules under which intentional, unintentional, or incidental radiators may operate. *See generally* 47 C.F.R. Part 15. Mobile devices, as intentional radiators (*see* 47 C.F.R. § 15.3(o)), are subject to Part 15's equipment authorization requirements. Specifically, unlicensed intentional radiators must be verified pursuant to the procedures in 47 C.F.R. Part 2, Subpart J. *See* 47 C.F.R. § 2.901 *et. seq.*

These rules are currently designed solely to prevent harmful interference to radio communications. Part 15, however, was adopted pursuant to the Commission's Section 302a authority which is not limited exclusively to preventing harmful interference.

Section 302a states:

[t]he Commission may, consistent with the *public interest*, convenience, and necessity, make reasonable regulations (1) *governing the interference potential* of devices which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause harmful interference to radio communications . . .

47 U.S.C. § 302a (emphasis added).

While Section 302a refers to "interference," the language is quite broad in that it covers any regulation, consistent with the public interest, governing interference potential. It is not limited to harmful interference, and it is not limited to actual interference; rather, it extends to interference "potential." *Id.*

Any regulation, consistent with the public interest, which impacts the interference potential of a Part 15 device is within the scope of Section 302a. Thus, a technology that limits the operation

of a mobile phone device (i.e. its ability to emit radio signals) in a particular environment is likely within the scope of Section 302a.

Try Safety First's Securitized Prison Protocol regulates the interference potential of mobile devices in that it limits their ability to emit radio signals, signals that have the potential to interfere with radio communications. That a device does not actually interfere with radio communications does not mean it evades FCC jurisdiction.

The legislative history of Section 302a acknowledges this well understood fact. Prior to the passage of Section 302a, the Commission only had the power "to prohibit the use of equipment or apparatus which causes interference to radio communications." 1968 *U.S. Code Cong. and Admin. News*, p. 2487. In other words, the FCC had no authority to attempt to regulate the interference potential of devices at the manufacturing level, but rather could only take action against a user of equipment when an actual instance of harmful interference had occurred. *See id.* at pp. 2487–2488. It was the Senate's view that it was more equitable to place the burden of equipment compliance on the manufacturer in the first instance. *See Id.*

The Commission has broad discretion in making policy determinations through the enactment of rules, and addressing the issue of contraband mobile phone use in prisons is squarely within the Commission's delegated authority and public safety responsibilities. *See American Radio Relay League, Inc. v. F.C.C.*, 617 F.2d 875, 881 (D.C. Cir. 1980) ("The Commission has broad discretion in making policy determinations through the enactment of rules;" denying a challenge to FCC rules prohibiting the manufacture and sale of certain amplifiers in order to combat the problem of radio interference with television reception); 47 U.S.C. §§ 151 - Purposes of chapter; Federal Communications Commission created (providing that the Commission was created for, among others, "the purpose of promoting safety of life and property through the use of wire and radio communications").

The Commission's authority to implement these regulations is further evidenced in the Commissions July 2015 NPRM, "Equipment Authorization and Electronic Labeling for Wireless Devices." *See* FCC NPRM 15-92, Equipment Authorization and Electronic Labeling for Wireless Devices, 80 Fed. Reg. 46900-01 (July 17, 2015). The purpose of that NPRM was to update the rules governing the evaluation and approval of RF devices.¹ This NPRM proposes "rules [that] would require any RF device that uses software to control its defining parameters to incorporate software security features that permit only those parties that have been authorized by the

¹ An RF device is any device that is capable of emitting RF energy by radiation, conduction, induction or other means. As defined in FCC rules, this includes radio communication transmitting devices and any device that includes a part or component that can act as an RF device. *See* 47 C.F.R. § 2.801. While RF devices generate RF energy, many devices do not generate it intentionally – that is, they are not communications devices but they generate RF emissions as a byproduct of their design. Such devices are defined as incidental or unintentional radiators. *See* 47 C.F.R. § 15.1.

manufacturer to make changes to the device's technical parameters." FCC NPRM 15-92, Equipment Authorization, at 7732.

The security features proposed by the FCC in this NPRM implicate similar policy goals and similar methods that Try Safety First now urges the FCC to adopt. The FCC recognizes that it may require manufactures to implement safety features related to wireless communication. These same methods can be used to solve the serious problem of contraband wireless device use in prisons.

2. The FCC's Ancillary Authority

While Section 302a alone provides sufficient authority to promulgate rules implementing the Try Safety First technology, the Commission may also utilize its ancillary authority. *See generally* 47 U.S.C. § 154(i).

The Commission has the authority to promulgate regulations to effectuate the goals and provisions of the Act even in the absence of an explicit grant of regulatory authority, if the regulations are reasonably ancillary to the Commission's specific statutory powers and responsibilities. *See* 47 U.S.C. § 154(i) (providing that the "Commission may perform *any and all acts*, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions.") (emphasis added).

In order for the Commission to regulate under its ancillary jurisdiction, two conditions must be met. First, the subject of the regulation must be covered by the Commission's general grant of jurisdiction under Title I of the Act. Second, the subject of the regulation must be "reasonably ancillary to the effective performance of the Commission's various responsibilities." *See United States v. Southwestern Cable Co.*, 392 U. S. 157 (1968).

Both of these conditions are satisfied here as: (1) mobile devices (intentional radiators) are covered by the FCC's Title I general jurisdictional grant; and (2) Automated Protocol Intelligence (API) regulations are reasonably ancillary to the Commission's regulatory authority over communication by wire or radio.

Furthermore, the statutorily proscribed policy goal of "promoting safety of life and property" is directly at issue. Both Section 151 – "Purposes of chapter; Federal Communications Commission created" and Section 154 – "Use of communications in safety of life and property" detail broad policy goals to promote public safety. *See* 47 U.S.C. §§ 154(o) ("For the purpose of obtaining maximum effectiveness from the use of radio and wire communications in connection with safety of life and property, the Commission shall investigate and study all phases of the problem and the best methods of obtaining the cooperation and coordination of these systems."); 332(a)(1) ("In taking actions to manage the spectrum to be made available for use by the private mobile service, the Commission shall consider, consistent with section 1 of this Act, whether such actions will . . . promote the safety of life and property.").

In other words, the FCC's broad ancillary authority – in addition to the other authority discussed above – empowers the Commission to continuously investigate and regulate new public safety problems created by technological advances in mobile technologies and the continuing increase in their use by inmates to carry on criminal enterprises from within the confines of correctional facilities.

IV. CONCLUSION

There is a significant public interest in preventing prisoners from using contraband wireless devices in prisons. New technology now allows the Commission to comprehensively and ubiquitously resolve this significant problem. The broad authority delegated to the FCC in Sections 332 and 302a, together with the FCC's ancillary authority under Section 154(i), provide Try Safety First with a strong argument that the FCC has the authority to mandate Try Safety First's Securitized Prison Protocol technology and finally solve this issue.